P21
G3

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-156772
(43)Date of publication of application : 08.06.2001

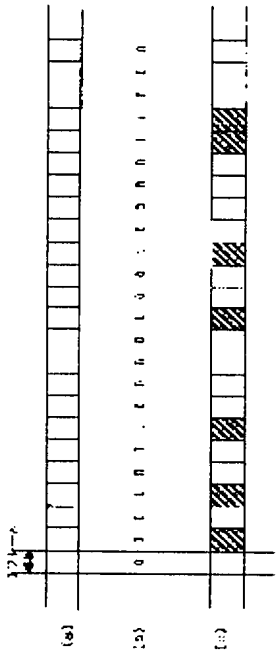
(51)Int.Cl. H04L 9/16
G06F 12/14
H04L 9/18
// G11B 20/10

(21)Application number : 11-339527
(22)Date of filing : 30.11.1999

(71)Applicant : VICTOR CO OF JAPAN LTD
(72)Inventor : KOHARI HARUKUNI

(54) ENCRYPTED INFORMATION REPRODUCTION METHOD AND ENCRYPTED INFORMATION REPRODUCTION DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an encrypted information reproduction method that can strongly prevent illegal use of contents information even in the case that a transmission stream is partially encrypted and to provide an encrypted information reproduction device.
SOLUTION: All audio or image stream is encrypted at random in the unit of frames on the basis of a random number generated by a specific generation polynomial and the encrypted stream is transmitted. Since flag information or the like denoting which stream is encrypted or not is not provided in the stream, the security strength against the illegal use of contents can be much more enhanced than that of a conventional partial encryption method. In the case of reproduction, a random number is obtained by the generation polynomial known by only a legal user, the encrypted frame is identified and the transferred stream is reproduced.



CLAIMS

[Claim(s)]
[Claim 1]A frame which enciphers, and a frame which is not enciphered are determined based on a random number generated using a predetermined generating polynomial, Data of a frame determined that it will encipher is an encipherment information regeneration method which reproduces a stream enciphered in each frame unit, An encipherment information regeneration method characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on a random number generated using said predetermined generating polynomial.
[Claim 2]Data of a frame which a frame which enciphers, and a frame which is not enciphered were determined based on a random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. It is an encipherment information regeneration method which reproduces a stream to which generating polynomial encipherment information as which information on said predetermined generating polynomial was enciphered was added, An encipherment information regeneration method characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on a random number generated using said generating polynomial obtained by solving a code of said generating polynomial encipherment information.
[Claim 3]Data of a frame which a frame which enciphers, and a frame which is not enciphered were determined based on a random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. Generating polynomial encipherment information as which information on said predetermined generating polynomial was enciphered, It is an encipherment information regeneration method which reproduces a stream to which initial value encipherment information as which information on two or more initial values for a random number generation of said predetermined generating polynomial was enciphered was added, Solve a code of said generating polynomial encipherment information, and restore said generating polynomial, and. A random number which solves a code of said initial value encipherment information, restores said initial value, and is generated using said restored generating polynomial, An encipherment information regeneration method characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on said restored initial value.
[Claim 4]A frame which enciphers, and a frame which is not enciphered are determined based on a random number generated using a predetermined generating polynomial, Data of a frame determined that it will encipher is encipherment information playback equipment which reproduces a stream enciphered in each frame unit, Encipherment information playback equipment characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on a random number generated using said predetermined generating polynomial.
[Claim 5]Data of a frame which a frame which enciphers, and a frame which is not enciphered were determined based on a random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. It is encipherment information playback equipment which reproduces a stream to which generating polynomial encipherment information as which information on said predetermined generating polynomial was enciphered was added, Encipherment information playback equipment characterized by reproducing a

stream after specifying a frame which is not enciphered as an enciphered frame based on a random number generated using said generating polynomial obtained by solving a code of said generating polynomial encipherment information.

[Claim 6]Data of a frame which a frame which enciphers, and a frame which is not enciphered were determined based on a random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. Generating polynomial encipherment information as which information on said predetermined generating polynomial was enciphered, It is encipherment information playback equipment which reproduces a stream to which initial value encipherment information as which information on two or more initial values for a random number generation of said predetermined generating polynomial was enciphered was added, Solve a code of said generating polynomial encipherment information, and restore said generating polynomial, and. A random number which solves a code of said initial value encipherment information, restores said initial value, and is generated using said restored generating polynomial, Encipherment information playback equipment characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on said restored initial value.

[Claim 7]Data of a frame which a frame which enciphers, and a frame which is not enciphered were determined based on a random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. A random number which is an encipherment information regeneration method which reproduces a stream to which information on two or more initial values for a random number generation of said predetermined generating polynomial was added, reproduces information on said initial value, acquires said initial value, and is generated using said generating polynomial, An encipherment information regeneration method characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on said reproduced initial value.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the encipherment information regeneration method and playback equipment for reproducing streams enciphered and transmitted, such as a sound and a picture. And an object of especially this invention is to provide the encipherment information regeneration method and playback equipment which prevent the unauthorized use of music, video information, etc. by enciphering streams, such as a sound and a picture, selectively and playing the stream to which processing made the encryption part hard to find was performed.
[0002]
[Description of the Prior Art]As for a low rate circuit like the Internet, progress of the compression technology of these days is enabling it to transmit music and a video signal by high definition. Based on such a background, distribute information business, such as music and an image, is spreading quickly. Although it is very convenient that high-definition music and video information can be easily obtained using the Internet, on the other hand, the unauthorized use of copying these information in large quantities without an owner's of a copyright permission poses a problem.
[0003]As a method of preventing the illicit copy of information, including music, an image, etc., many methods of enciphering the information itself are adopted from the former. That is, since it cannot return to the original information even if copied unjustly if the key used for encryption is not known, it is a method kept as a copy which is completely meaningless as a result.
[0004]An example of information transmission using the enciphering method currently performed conventionally is shown in drawing 3. If the line connection of a user (receiver) and a provider (transmitting side) is performed, authenticating processing will be made first (Step 1). When a receiver is judged as a result of attestation to be (NG) which is not a registered user, it is natural, but a circuit is intercepted there. If judged with (O.K.) which is a registered user, contents information enciphered as the key (key) used when enciphering contents information, such as music and an image, will be transmitted to the user side (Steps 2-4).
[0005]Here, although it is transmission of the key used when enciphering contents information, a key also gives and transmits not a state (nakedness) as it is but a certain encryption. Special data (ID) is used for the key for enciphering a key. For example, there are a system ID, a membership number, etc. which are data peculiar to the reception (user) side. Or data not to tell is also effective in others, such as a credit card number and an ATM card number, as ID.
[0006]The key which acquired such ID and was enciphered is expressed as Ex (ID, Key), as shown in drawing 3. It means enciphering by certain cipher system Ex() by using as a key ID which mentioned above Key which is a key for enciphering music information and video information. It will be set to Ey (Key, Data) if encryption of music or video information (Data) is expressed using the same formula.
[0007] Ey (Key, Data) which is the information on a sound or an image enciphered as Ex (ID, Key) which is the enciphered key will be memorized by the receiver. Any data is enciphered, and even if copied unjustly, it cannot return to the original music or video information easily. The above is an outline of the method taken in order to prevent the unauthorized use of the information on the former.
[0008]

[Problem(s) to be Solved by the Invention]By the way, for raising a user's buying will, even if, also in the state of inferior quality, a part of music used as a purchase object and image are followed, as it can play freely, and it is advantageous Lycium chinense and (to change into the state where it does not encipher) in respect of being various. In order that becoming a problem here may prevent an unauthorized use, when enciphering to the whole contents, it is a thing which do not solve a code thoroughly and for which it cannot restrict and neither music nor an image can be played at all.
[0009]On the other hand, in order to enable partial reproduction in the quality of the grade which has not solved a code, either, when enciphering selectively, the information (flag) on which portion of the stream is enciphered conventionally was provided in the inside of Stream transmitted. Therefore, it becomes easy to return the whole contents to the original information, and there was a problem that the capability to prevent an unauthorized use declined.
[0010]Even if this invention does not solve reproduction in a certain amount of partial quality of transmission streams, such as a sound and a picture, a code, in order that it may enable, It aims at providing the encipherment information regeneration method and playback equipment which can prevent the unauthorized use of KONDENTSU powerfully, when a transmission stream is enciphered selectively.
[0011]
[Means for Solving the Problem]Then, in order to solve an aforementioned problem, this invention provides following the (1) - (7).
(1) A frame which enciphers, and a frame which is not enciphered are determined based on a random number generated using a predetermined generating polynomial, Data of a frame determined that it will encipher is an encipherment information regeneration method which reproduces a stream enciphered in each frame unit, An encipherment information regeneration method characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on a random number generated using said predetermined generating polynomial.
(2) Data of a frame which a frame which enciphers, and a frame which is not enciphered were determined based on a random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. It is an encipherment information regeneration method which reproduces a stream to which generating polynomial encipherment information as which information on said predetermined generating polynomial was enciphered was added, An encipherment information regeneration method characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on a random number generated using said generating polynomial obtained by solving a code of said generating polynomial encipherment information.
(3) Data of a frame which a frame which enciphers, and a frame which is not enciphered were determined based on a random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. Generating polynomial encipherment information as which information on said predetermined generating polynomial was enciphered, It is an encipherment information regeneration method which reproduces a stream to which initial value encipherment information as which information on two or more initial values for a random number generation of said predetermined generating polynomial was enciphered was added, Solve a code of said generating polynomial encipherment information, and restore said generating polynomial, and. A random number which solves a code of said initial value encipherment information, restores said initial value, and is generated using said restored generating polynomial, An encipherment information regeneration method characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on said restored initial value.
(4) A frame which enciphers, and a frame which is not enciphered are determined based on a random number generated using a predetermined generating polynomial, Data of a frame determined that it will encipher is encipherment information playback equipment which reproduces a stream enciphered in each frame unit, Encipherment information playback equipment characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on a random number generated using said predetermined generating polynomial.
(5) Data of a frame which a frame which enciphers, and a frame which is not enciphered were determined based on a random number generated using a predetermined generating polynomial, and

was determined that it will encipher is enciphered in each frame unit, and. It is encipherment information playback equipment which reproduces a stream to which generating polynomial encipherment information as which information on said predetermined generating polynomial was enciphered was added, Encipherment information playback equipment characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on a random number generated using said generating polynomial obtained by solving a code of said generating polynomial encipherment information.
(6) Data of a frame which a frame which enciphers, and a frame which is not enciphered were determined based on a random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. Generating polynomial encipherment information as which information on said predetermined generating polynomial was enciphered, It is encipherment information playback equipment which reproduces a stream to which initial value encipherment information as which information on two or more initial values for a random number generation of said predetermined generating polynomial was enciphered was added, Solve a code of said generating polynomial encipherment information, and restore said generating polynomial, and. A random number which solves a code of said initial value encipherment information, restores said initial value, and is generated using said restored generating polynomial, Encipherment information playback equipment characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on said restored initial value.
(7) Data of a frame which a frame which enciphers, and a frame which is not enciphered were determined based on a random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. A random number which is an encipherment information regeneration method which reproduces a stream to which information on two or more initial values for a random number generation of said predetermined generating polynomial was added, reproduces information on said initial value, acquires said initial value, and is generated using said generating polynomial, An encipherment information regeneration method characterized by reproducing a stream after specifying a frame which is not enciphered as an enciphered frame based on said reproduced initial value.
[0012]
[Embodiment of the Invention]The encryption disposal method of the stream in one example of an encipherment information transmission method is shown in drawing 1. Drawing 1 (a) shows the frame in a sound or an imaged stream. When voice data is linear PCM, there may be no concept of a frame into a stream, but the concept of a frame can be easily introduced by making hundreds - the data for thousands samples into one frame, and inserting a frame alignment signal in the head.
[0013]It is general because of saving of transmission according to compression audio or a compressed image by progress of the compression technology of these days of a transmission time. In the case of compression audio data, the concept of the frame is always introduced, if it is compression by a fixed rate, each frame will serve as the same size, and if it is a variable rate, it will become different size for every frame. In the case of compressed image streams, although based also on compression technology, it becomes with generally different size for every frame in many cases. Anyway, since the size of a frame is not the contents of this invention, and directly related, in drawing 1, the same size shows it.
[0014]Here, the random number value generated by the specific generating polynomial is shown in drawing 1 (b). When a random number value is "0", encryption of the frame is not performed, but the frame shall be enciphered when a random number value is "1." A sound or an imaged stream is enciphered at random per frame based on a random number value, as shown in drawing 1 (c).
[0015]If such processing is performed, unless a code is restored, it is clear that a normal sound or picture are not reproduced. Since the data (Data (n)) of the enciphered frame is expressed as Ey (Key, Data (n)), it enciphers key (Key) using ID like a conventional system to maintain safe intensity. The enciphered key information is expressed as Ex (ID, Key), and safe intensity is the same as a conventional system. The focus here is whether enciphered per frame. Since handicraft processing whether to solve a code for every frame of a stream will be required even if the key (Key) is stolen, in order to return the whole information to the state of perfect origin, it is clear that remarkable time and effort is needed. Thus, since it makes it hard to find out where the portion enciphered is, this example

can raise the safe intensity to the unauthorized use of contents rather than the conventional partial encryption method. [it]

[0016]Next, the random number generation used for the determination of whether to encipher is explained. Since generating of a random number is easily realizable by the M sequence signal generator and soft processing based on a generating polynomial specific like the wisdom of the many, although detailed explanation is excluded, it is a meaning which secures safety about the degree of a generating polynomial, and is good to determine in consideration of the following points.

[0017]If the degree of a generating polynomial is set to m now, the random number generated will be patrolled by 2^m-1 time. Therefore, it is desirable to set up the degree m so that "2^m-1" may become a sufficiently bigger value than the total frame number of a sound or an imaged stream. For example, if frame frequency shall be 100 Hz from contents of 2 hours, the total frame number will be set to 7200 second x100=720k. Therefore, m is enough if it is made or more into 20. Since the kind of specific generating polynomial which can generate a random number also increases the more the more the degree m becomes high, supposing it is m= 20, for example, it will become a situation already next to impossible to find out the generating polynomial actually used.

[0018]In this example, in order to raise safe intensity, it is making to encipher and transmit also about the generating polynomial for a random number generation into the feature. Generating polynomial type encryption can be expressed as Ez (ID, generating polynomial). Even if it makes cipher system Ez() here the same as cipher system Ex() when coincidence-izing the key (Key), it is satisfactory, but if it is going to raise safe intensity, it is also possible to change a cryptographic algorithm.

[0019]As mentioned above, the encryption transmission method of streams, such as a sound, a picture, etc. in this example, It is [whether an applicable frame is enciphered and] determination sushi ****** based on the random number generated by a specific generating polynomial, without establishing in a stream the flag information etc. which not the whole but show a stream for which frame it enciphers selectively and is enciphered. In order to secure safety, the information about the used generating polynomial is enciphered and it transmits to a receiver.

[0020]The flow of these processings is shown in drawing 2. the data Ey (Key, Data (n)) which enciphered the data Ex (ID, Key) which enciphered the key (Key), the sound, and the imaged stream in drawing 2 -- in addition, the data Ez (ID, generating polynomial) which enciphered the type of the generating polynomial for a random number generation is transmitted to the receiver. Although "transmission of the initial value table for a random number generation" is indicated to Step 14 of drawing 2, about this, details are mentioned later.

[0021]If drawing 2 is explained briefly and the line connection of a user (receiver) and a provider (transmitting side) will be performed, authenticating processing will be made first (Step 1). When a receiver is judged as a result of attestation to be (NG) which is not a registered user, it is natural, but a circuit is intercepted there. If judged with (O.K.) which is a registered user, in Step 12, the key (ID) for enciphering the type of the key (Key) and a generating polynomial will be acquired, and the data Ex (ID, Key) and Ez (ID, generating polynomial) which enciphered the type of the key (Key) and the generating polynomial will be obtained. In Step 13, acquisition or a random number is generated for the data Ey (Key, Data (n)) which enciphered contents information, such as a sound and a picture, and the data Ey (Key, Data (n)) is generated. Ey (Key, Data (n)) which is the data (what naturally also contains the data of the frame which is not enciphered as shown in drawing 1 (C)) which enciphered contents information in Step 14 -- in addition, Ex (ID, Key) and Ez (ID, generating polynomial) -- the data of the initial value table (two or more initial values for a random number generation) for a random number generation is further transmitted to a receiver.

[0022]In the data Ez (ID, generating polynomial) which enciphered the type of the generating polynomial for the data Ex (ID, Key) which enciphered the key (Key), and a random number generation, although the key for encryption serves as the same ID, Since mutually different information may be used, how to use a system ID for ID of Ex (ID, Key), and to use an ATM card number for ID of Ez (ID, generating polynomial) can be considered, for example.

[0023]As a transmission medium which delivers the information from the transmission side to a receiver (reproduction side), Since it is big capacity even if the transmission stream Ey (Key, Data (n)) of the enciphered sound or a picture is condensed information, recording media, such as not only

circuits (an optical cable, an electrical signal cable, etc.) but an optical disc and a magnetic recording medium, may be used.

[0024]As encipherment information transmission equipment which realizes processing shown in drawing 2, A means to determine the frame which enciphers to the stream which consists of two or more frames based on the random number generated using a predetermined generating polynomial, and the frame which is not enciphered, A means to encipher the data of the frame determined that it will encipher in each frame unit, A means to generate the generating polynomial encipherment information which enciphered the information on said predetermined generating polynomial, The encipherment information transmission equipment provided with a means to transmit a means to generate the initial value encipherment information which enciphered the information on two or more initial values for the random number generation of said predetermined generating polynomial, the stream which enciphered selectively, generating polynomial encipherment information, and initial value encipherment information can be considered.

[0025]By the way, the method of not establishing in a stream the flag information etc. which show whether it is the frame which enciphers a stream selectively per frame and is enciphered as having mentioned above is very excellent in the field of the safe intensity to an unauthorized use. However, in reproducing from the middle of a stream, there are the following disadvantageous fields. Namely, since generating of the random number which determines whether encipher or not is continuously performed per frame, if it is going to reproduce from the middle of a stream suddenly, the random number generation from the frame of the beginning of a stream to an intermediate frame (namely, -- up to the frame which starts reproduction) must be performed for a short time. This is dramatically difficult.

[0026]By this example, in order to solve this problem, as shown in Step 14 of drawing 2 mentioned above, two or more initial values for the random number generation computed beforehand are prepared (preparing an initial value table), and it transmits to a receiver. every [for example,] 100 frames -- that is, if frame frequency is 100 Hz, it will become a random number value in one second bit. Since one initial value is the size of m bit when the degree of the generating polynomial for a random number generation is set to m, for example to contents of 2 hours, an initial value table serves as a 7200*m bit. When reproducing from the middle of a stream, since it understands what present frame there is from the beginning easily, with a frame address, a time code, etc., If the optimal initial value is chosen from an initial value table and it is set as a random number generator, it will become possible to have a random number generator in a desired state by the very slight number of steps.

[0027]Thus, it becomes more nearly renewable than the arbitrary positions of a stream also by the method of not establishing the flag information etc. which encipher a stream selectively and show whether it being the frame enciphered in a stream. When transmitting the initial value (initial value table) of these plurality to a receiver, it may transmit as it is, but it is clear that it is safer to encipher and transmit.

[0028]In the transmission method which the above explanation enciphers a stream selectively and does not establish the flag information etc. which show whether it is the frame enciphered in a stream, In order to make it possible to reproduce from the middle of a stream easily, the method of transmitting the initial value table for a random number generation from the transmitting side was introduced.

[0029]When the generating polynomial for a random number generation is known a priori by the receiver (reproduction side) which is a regular user, it is possible to create an initial value table in advance of reproduction of a transmission stream. Or it is also possible to create not an initial value table but the random number value itself. Because, since a random number value is 1 bit of "0" and "1", it is realizable size even if it creates the random number table for the total frame. For example, if frame frequency shall be 100 Hz from contents of 2 hours, the total frame number will be 7200x100=720k bit =90 K byte.

[0030]On the other hand, in the case of the initial value table mentioned above, if it tends to be considered as the degree m= 20 of a generating polynomial and is going to create the initial value table in every 100 frames, it will become with 7200x100x20 / 100 bits = 18 K bytes. Although the direction which transmitted or created the initial value table considering the field of the memory size in a receiver (reproduction side) is excellent, it seems that the direction of the random number table corresponding to the total frame generated by a receiver is excellent in user-friendliness. Anyway, reproduction from the middle of a transmission stream can be performed easily, securing the safe

intensity to an unauthorized use.
[0031]Here, the following methods can be considered about the regeneration method (receiving method) of a transmission stream mentioned above.
(b) The frame which enciphers, and the frame which is not enciphered are determined based on the random number generated using a predetermined generating polynomial, The data of the frame determined that it will encipher is an encipherment information regeneration method which reproduces the stream enciphered in each frame unit, An encipherment information regeneration method characterized by reproducing a stream after specifying the frame which is not enciphered as the enciphered frame based on the random number generated using said predetermined generating polynomial.
(**) The data of the frame which the frame which enciphers, and the frame which is not enciphered were determined based on the random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. It is an encipherment information regeneration method which reproduces the stream to which the generating polynomial encipherment information as which the information on said predetermined generating polynomial was enciphered was added, An encipherment information regeneration method characterized by reproducing a stream after specifying the frame which is not enciphered as the enciphered frame based on the random number generated using said generating polynomial obtained by solving the code of said generating polynomial encipherment information.
(**) The data of the frame which the frame which enciphers, and the frame which is not enciphered were determined based on the random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. The generating polynomial encipherment information as which the information on said predetermined generating polynomial was enciphered, It is an encipherment information regeneration method which reproduces the stream to which the initial value encipherment information as which the information on two or more initial values for the random number generation of said predetermined generating polynomial was enciphered was added, Solve the code of said generating polynomial encipherment information, and restore said generating polynomial, and. The random number which solves the code of said initial value encipherment information, restores said initial value, and is generated using said restored generating polynomial, An encipherment information regeneration method characterized by reproducing a stream after specifying the frame which is not enciphered as the enciphered frame based on said restored initial value.
(**) The data of the frame which the frame which enciphers, and the frame which is not enciphered were determined based on the random number generated using a predetermined generating polynomial, and was determined that it will encipher is enciphered in each frame unit, and. The random number which is an encipherment information regeneration method which reproduces the stream to which the information on two or more initial values for the random number generation of said predetermined generating polynomial was added, reproduces the information on said initial value, acquires said initial value, and is generated using said generating polynomial, An encipherment information regeneration method characterized by reproducing a stream after specifying the frame which is not enciphered as the enciphered frame based on said reproduced initial value.
[0032]As encipherment information playback equipment which realizes the above-mentioned regeneration method, A means to solve the code of said generating polynomial encipherment information, and to restore said generating polynomial, A means to solve the code of said initial value encipherment information, and to restore said initial value, and the random number generated using said restored generating polynomial, Based on said restored initial value, encipherment information playback equipment provided with ****** which reproduces a stream based on the information on the existence of the encryption after a means to specify the frame which is not enciphered as the enciphered frame, and ** as which the existence of the encryption for every frame was specified can be considered.
[0033]
[Effect of the Invention]According to [above passage] this invention, the whole contents information, such as a sound and a picture, is not enciphered and it is enciphered selectively and at random, And since the transmission stream which it is made hard to find out which portion the portion enciphered is is reproduced, reproduction which raised the safe intensity to the unauthorized use of contents can be

performed. [it] Since the information enciphered selectively and at random without enciphering the whole contents information is reproduced, it is very advantageous to being able to perform freely partial reproduction in a certain amount of quality, and making a user's buying will increase. When reproducing the transmission stream to which the information on two or more initial values for the random number generation of a predetermined generating polynomial was added, in the time of reproduction, reproduction from the middle of a transmission stream can be performed easily, securing the safe intensity to an unauthorized use.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a figure showing encryption processing of the transmission stream treated in the one example of the encipherment information regeneration method in this invention.
[Drawing 2]It is a figure showing the flow of the transmission stream generation treated in the one example of the encipherment information regeneration method in this invention.
[Drawing 3]It is a figure showing the conventional encipherment information transmission method.

[Translation done.]

DRAWINGS

[Drawing 1]

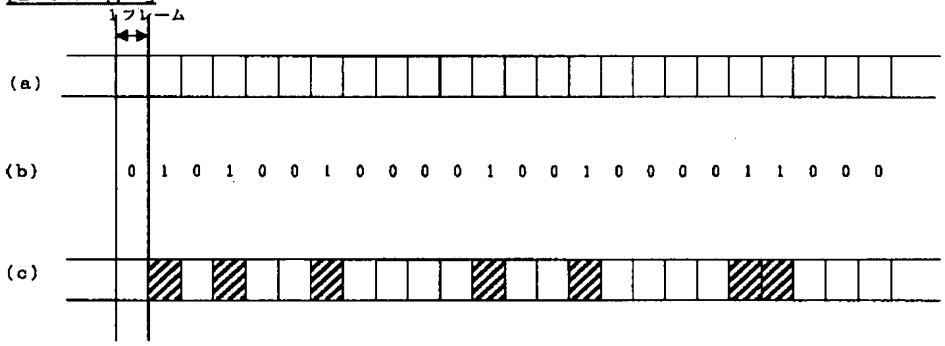


図1

[Drawing 2]

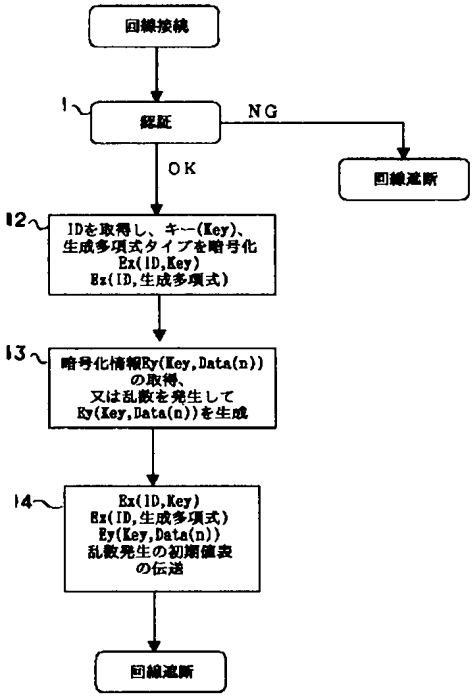


図2

[Drawing 3]

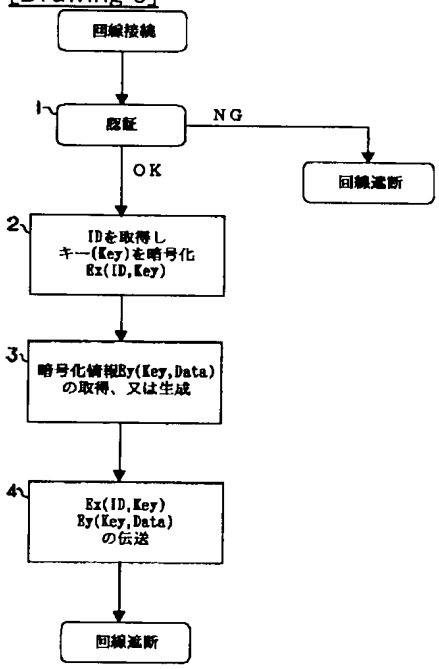


図3

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－156772
（P2001－156772A）
(43)公開日　平成13年６月８日(2001.6.8)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/16		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ１１Ｂ　20/10	Ｈ	５Ｄ０４４
Ｈ０４Ｌ　9/18		Ｈ０４Ｌ　9/00	６４３	５Ｊ１０４
// Ｇ１１Ｂ　20/10			６５１	

審査請求　未請求　請求項の数７　ＯＬ　（全８頁）

(21)出願番号　特願平11－339527

(22)出願日　平成11年11月30日(1999.11.30)

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地
(72)発明者　小張　晴邦
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

Ｆターム(参考)　5B017 AA07 BA05 BA07 CA06 CA09 CA16
5D044 AB05 AB07 DE03 DE48 CK17 HL11
5J104 AA33 JA04

(54)【発明の名称】　暗号化情報再生方法及び暗号化情報再生装置

(57)【要約】
【課題】　伝送ストリームを部分的に暗号化した場合においても、コンデンツ情報の不正使用を強力に防止できる暗号化情報再生方法及び再生装置を提供すること。
【解決手段】　音声または画像ストリームは、特定の生成多項式により発生される乱数値に基づきフレーム単位でランダムに暗号化され伝送される。どのフレームが暗号化されているか否かを示すフラッグ情報などをストリーム内に設けていないので、コンテンツの不正使用に対する安全強度を、従来の部分的な暗号化方法よりも高めることができる。再生時には、正規ユーザーのみが知り得る前記生成多項式により乱数値を得て暗号化されているフレームを特定し、転送ストリームを再生する。

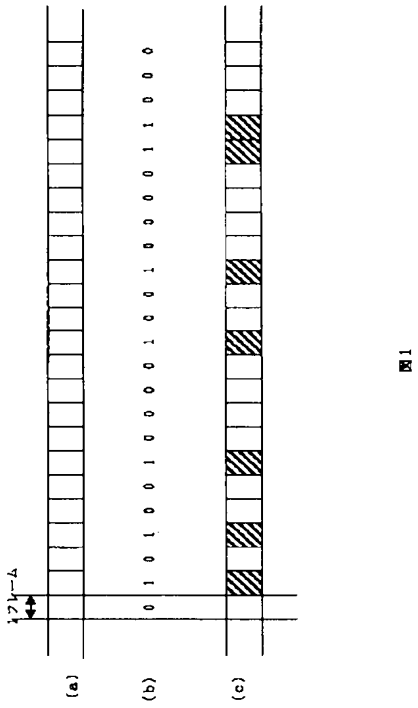


図1

【特許請求の範囲】
【請求項１】所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されたストリームを再生する暗号化情報再生方法であって、
前記所定の生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。
【請求項２】所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報が付加されたストリームを再生する暗号化情報再生方法であって、
前記生成多項式暗号化情報の暗号を解き、得られた前記生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。
【請求項３】所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の初期値の情報が暗号化された初期値暗号化情報とが付加されたストリームを再生する暗号化情報再生方法であって、
前記生成多項式暗号化情報の暗号を解き前記生成多項式を復元すると共に、前記初期値暗号化情報の暗号を解き前記初期値を復元し、
復元された前記生成多項式を用いて発生される乱数と、復元された前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。
【請求項４】所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されたストリームを再生する暗号化情報再生装置であって、
前記所定の生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生装置。
【請求項５】所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報が付加されたストリームを再生する暗号化情報再生装置であって、
前記生成多項式暗号化情報の暗号を解き、得られた前記生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生装置。
【請求項６】所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の初期値の情報が暗号化された初期値暗号化情報とが付加されたストリームを再生する暗号化情報再生装置であって、
前記生成多項式暗号化情報の暗号を解き前記生成多項式を復元すると共に、前記初期値暗号化情報の暗号を解き前記初期値を復元し、
復元された前記生成多項式を用いて発生される乱数と、復元された前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生装置。
【請求項７】所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の乱数発生のための複数の初期値の情報が付加されたストリームを再生する暗号化情報再生方法であって、
前記初期値の情報を再生して前記初期値を得、前記生成多項式を用いて発生される乱数と、再生した前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、暗号化して伝送された音声や画像等のストリームを再生するための暗号化情報再生方法及び再生装置に関するものである。そして、この発明は特に、音声や画像等のストリームが部分的に暗号化され、かつ暗号化箇所を見つけ難くした処理を施されたストリームを再生することによって、音楽や映像情報等の不正使用を防止する暗号化情報再生方法及び再生装置を提供することを目的とする。
【０００２】

【従来の技術】昨今の圧縮技術の進歩により、インターネットのような低レートな回線でも音楽や映像信号を高品位で伝送することが可能となってきている。このような背景をもとに、音楽や映像などの情報配信ビジネスが急速に普及しつつある。インターネットを利用して、簡単に高品位な音楽や映像情報を入手できることは大変便利ではあるが、一方ではこれらの情報を著作権者の許可なく大量に複写するなどの不正使用が問題となっている。

【０００３】音楽や映像等の情報の不正複写を防止する方法としては、情報そのものを暗号化する方法が従来から数多く採用されている。つまり、暗号化に使用した鍵が解らなければ、仮に不正に複写されても元の情報に戻せないので、結果的に全く意味のない複写としてしまう方式である。

【０００４】図３に、従来より行われている暗号化手法を用いた情報伝送の一例を示す。ユーザー（受信側）とプロバイダー（送信側）との回線接続が行われると、まず最初に認証処理がなされる（ステップ１）。認証の結果、受信側が正規ユーザーではない（ＮＧ）と判定されると、当然のことであるが、そこで回線が遮断される。正規ユーザーである（ＯＫ）と判定されると、コンテンツ情報を暗号化するときに使用したキー（鍵）と暗号化された音楽、映像等のコンテンツ情報がユーザー側に伝送される（ステップ２～４）。

【０００５】ここで、コンテンツ情報を暗号化する際に使用したキーの伝送であるが、キーもそのままの状態（裸）ではなく、何らかの暗号化を施して伝送する。キーを暗号化するためのキーには特殊なデータ（ＩＤ）が使用される。例えば、受信（ユーザー）側固有のデータであるシステムＩＤとか会員番号などがある。或いは、クレジットカード番号とかキャッシュカード番号というような他人には知らせたくないデータもＩＤとして有効である。

【０００６】このようなＩＤを取得して暗号化したキーは、図３に示したようにEx(ID,Key)と表現される。音楽情報や映像情報を暗号化するためのキーであるKeyを、前述したIDをキーとして、ある暗号化方式Ex()で暗号化するということを意味している。同様な式を用いて音楽や映像情報（Data）の暗号化を表現すると、Ey(Key,Data)となる。

【０００７】受信側には暗号化されたキーである Ex(ID,Key)と、暗号化された音声や映像の情報である Ey(Key,Data)が記憶されることになる。何れのデータも暗号化されており、仮に不正に複写されても簡単には元の音楽や映像情報に戻すことができないわけである。以上が、従来よりの情報の不正使用を防止するために採られている方式の概要である。

【０００８】

【発明が解決しようとする課題】ところで、ユーザの購入意欲を高めるに、購入対象となる音楽や映像の一部を、たとえ品質が悪い状態でも自由に再生できるようにしておいくこと（暗号化しない状態のままにしておくこと）は、いろいろな面で有利である。ここで問題となるのが、不正使用を防止するために、コンテンツ全体に暗号化を施した場合には、暗号を完全に解かない限り、全く音楽や映像を再生することができないことである。

【０００９】一方、暗号を解かなくてもある程度の品質で部分的な再生を可能とするために、部分的に暗号化を施した場合には、従来、ストリームのどの部分が暗号化されているか否かの情報（フラッグ）を、伝送されるストリーム内部に設けていた。よって、コンテンツ全体を元の情報に戻しやすくなり、不正使用を防止する能力が低下するといった問題があった。

【００１０】この発明は、音声や画像等の伝送ストリームの部分的なある程度の品質での再生を、暗号を解かなくても可能とするために、伝送ストリームを部分的に暗号化した場合においても、コンデンツの不正使用を強力に防止できる暗号化情報再生方法及び再生装置を提供することを目的とする。

【００１１】

【課題を解決するための手段】そこで、上記課題を解決するために本発明は、下記（１）～（７）を提供するものである。

（１）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されたストリームを再生する暗号化情報再生方法であって、前記所定の生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

（２）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報が付加されたストリームを再生する暗号化情報再生方法であって、前記生成多項式暗号化情報の暗号を解き、得られた前記生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

（３）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の

初期値の情報が暗号化された初期値暗号化情報とが付加されたストリームを再生する暗号化情報再生方法であって、前記生成多項式暗号化情報の暗号を解き前記生成多項式を復元すると共に、前記初期値暗号化情報の暗号を解き前記初期値を復元し、復元された前記生成多項式を用いて発生される乱数と、復元された前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

（４）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されたストリームを再生する暗号化情報再生装置であって、前記所定の生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生装置。

（５）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報が付加されたストリームを再生する暗号化情報再生装置であって、前記生成多項式暗号化情報の暗号を解き、得られた前記生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生装置。

（６）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の初期値の情報が暗号化された初期値暗号化情報とが付加されたストリームを再生する暗号化情報再生装置であって、前記生成多項式暗号化情報の暗号を解き前記生成多項式を復元すると共に、前記初期値暗号化情報の暗号を解き前記初期値を復元し、復元された前記生成多項式を用いて発生される乱数と、復元された前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生装置。

（７）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の乱数発生のための複数の初期値の情報が付加されたストリームを再生する暗号化情報再生方法であって、前記初期値の情報を再生して前記初期値を得、前記生成多項式を用いて発生される乱数と、再生した前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

【００１２】

【発明の実施の形態】図１に、暗号化情報伝送方法の一実施例におけるストリームの暗号化処理方法を示す。図１（ａ）は、音声または画像ストリーム内のフレームを示している。音声データがリニアＰＣＭの場合には、ストリーム内にフレームといった概念が無い場合もあるが、数百～数千サンプル分のデータを１フレームとして、その先頭にフレーム同期信号を挿入することにより、フレームの概念を容易に導入することができる。

【００１３】また、昨今の圧縮技術の進歩により、圧縮音声や圧縮画像による伝送が伝送時間の節約のために一般的となっている。圧縮音声データの場合には、必ずフレームの概念が導入されており、固定レートによる圧縮であれば各フレームは同一サイズとなり、可変レートであればフレーム毎に異なるサイズとなる。また、圧縮画像ストリームの場合には、圧縮方式にもよるが一般的にはフレーム毎に異なるサイズとなることが多い。何れにしても、フレームのサイズは本発明内容と直接関係ないので、図１においては同一サイズで示している。

【００１４】ここで、特定の生成多項式により発生された乱数値を図１（ｂ）に示す。乱数値が「０」のときはそのフレームの暗号化は行わず、乱数値が「１」のときはそのフレームの暗号化を行うものとする。音声または画像ストリームは、図１（ｃ）に示したように、乱数値に基づきフレーム単位でランダムに暗号化される。

【００１５】このような処理を施しておけば、暗号を復元しない限り正常な音声や画像が再生されないことは明らかである。暗号化されたフレームのデータ（Data(n)）は、Ey(Key,Data(n))と表現されるので、安全強度を保つには従来方式と同じようにキー（Key）をIDを用いて暗号化する。暗号化されたキー情報は、Ex(ID,Key)と表現され、安全強度は従来方式と同じである。ここでの特徴点は、フレーム単位で暗号化されているか否かである。仮に、キー（Key）が盗まれたとしても、ストリームのフレーム毎に暗号を解くか否かの手作業的な処理が要求されるので、情報全体を完全な元の状態に戻すには、かなりの手間が必要となることは明らかである。このように、本実施例は暗号化されている部分が何処であるか見つけ出し難くしているので、コンテンツの不正使用に対する安全強度を、従来の部分的な暗号化方法よりも高めることができる。

【００１６】次に、暗号化を行うか否かの決定に使用される乱数発生について説明する。乱数の発生は、衆知の如く、特定の生成多項式に基づくＭ系列信号発生器やソフト処理で容易に実現できるので、詳細説明は省くが、

生成多項式の次数については安全性を確保する意味で、次のような点を考慮して決定するとよい。

【００１７】今、生成多項式の次数をｍとすると、発生される乱数は2^m-1回で巡回する。従って、「2^m-1」が音声や画像ストリームの総フレーム数より十分大きな値となるように、次数ｍを設定することが望ましい。例えば、２時間のコンテンツで、フレーム周波数を１００Ｈｚとすると、総フレーム数は、７２００秒×１００＝７２０ｋとなる。従って、ｍは２０以上にすれば十分である。次数ｍが高くなればなるほど、乱数を発生できる特定の生成多項式の種類も増えるので、例えばｍ＝２０であるとすると、実際に使用されている生成多項式を見つけだすことはもはや不可能に近い状況となる。

【００１８】本実施例では、安全強度を高めるために、乱数発生のための生成多項式についても暗号化して伝送することを特長としている。生成多項式タイプの暗号化は、Ez(ID,生成多項式)と表現できる。ここでの暗号化方式 Ez()は、キー（Key）を暗合化するときの暗号化方式Ex()と同じにしても問題は無いが、少しでも安全強度を高めようとするならば、暗号アルゴリズムを変えることも可能である。

【００１９】以上のように、本実施例における音声・画像等のストリームの暗号化伝送方法は、ストリームを全体でなく部分的に暗号化し、かつ、どのフレームが暗号化されているか否かを示すフラッグ情報などをストリーム内に設けずに、特定の生成多項式により発生される乱数を基に、該当フレームを暗号化するか否かを決定すしている。さらに、安全性を確保するために、使用された生成多項式に関する情報を暗号化して受信側に伝送する。

【００２０】これらの処理のフローを、図２に示す。図２において、キー（Key）を暗号化したデータEx(ID,Key)、音声や画像ストリームを暗号化したデータEy(Key,Data(n))に加えて、乱数発生のための生成多項式のタイプを暗号化したデータEz(ID,生成多項式)を受信側に伝送している。なお、図２のステップ１４には「乱数発生のための初期値表の伝送」が記載されているが、これについては詳細を後述する。

【００２１】図２について簡単に説明すると、ユーザー（受信側）とプロバイダー（送信側）との回線接続が行われると、まず最初に認証処理がなされる（ステップ１）。認証の結果、受信側が正規ユーザーではない（ＮＧ）と判定されると、当然のことであるが、そこで回線が遮断される。正規ユーザーである（ＯＫ）と判定されると、ステップ１２において、キー（Key）及び生成多項式のタイプを暗号化するためのキー(ID)を取得し、キー（Key）及び生成多項式のタイプを暗号化したデータEx(ID,Key)とEz(ID,生成多項式)を得る。ステップ１３において、音声・画像等のコンテンツ情報を暗号化したデータEy(Key,Data(n))を取得、または、乱数を発生させてデータEy(Key,Data(n))を生成する。ステップ１４において、コンテンツ情報を暗号化したデータ（図１（Ｃ）に示すように暗号化されていないフレームのデータも当然含むもの）であるEy(Key,Data(n))に加えて、Ex(ID,Key)とEz(ID,生成多項式)、さらには乱数発生のための初期値表（乱数発生のための複数の初期値）のデータを受信側に伝送する。

【００２２】なお、キー（Key）を暗号化したデータEx(ID,Key)、乱数発生のための生成多項式のタイプを暗号化したデータEz(ID,生成多項式)において、暗号化のためのキーは同じＩＤとなっているが、お互いに異なる情報を用いてもかまわないので、例えば、Ex(ID,Key)のIDにはシステムＩＤを、Ez(ID,生成多項式)のIDにはキャッシュカード番号を使用するといった方法が考えられる。

【００２３】伝送側から受信側（再生側）への情報の受け渡しを行う伝送媒体としては、暗号化された音声や画像の伝送ストリームEy(Key,Data(n))が圧縮情報であっても大きな容量であるため、回線（光ケーブル、電気信号ケーブル等）ばかりでなく、光ディスクや磁気記録媒体といった記録媒体でもよい。

【００２４】図２に示す処理を実現する暗号化情報伝送装置としては、複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定する手段と、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化する手段と、前記所定の生成多項式の情報を暗号化した生成多項式暗号化情報を生成する手段と、前記所定の生成多項式の乱数発生のための複数の初期値の情報を暗号化した初期値暗号化情報を生成する手段と、部分的に暗号化を行ったストリームと生成多項式暗号化情報と初期値暗号化情報とを伝送する手段を備えた暗号化情報伝送装置が考えられる。

【００２５】ところで、前述したようにストリームをフレーム単位で部分的に暗号化し、かつ暗号化されているフレームであるか否かを示すフラッグ情報などをストリーム内に設けない方法は、不正使用に対する安全強度という面では大変優れている。但し、ストリームの途中から再生する場合には次のような不利な面がある。即ち、暗号化するか否かを決定する乱数の発生はフレーム単位で連続的に行われるため、いきなりストリームの途中から再生しようとすると、ストリームの最初のフレームから途中のフレームまで（即ち再生を開始するフレームまで）の乱数発生を短時間に行わなければならない。これは、非常に難しい。

【００２６】この問題を解決するために、本実施例では、前述した図２のステップ１４に示したように、前もって算出した乱数発生のための初期値を複数個用意し（初期値表を用意し）、受信側へ伝送する。例えば、１

００フレーム毎、即ち仮にフレーム周波数が１００Ｈｚであれば、１秒単位での乱数値となる。一つの初期値は、乱数発生のための生成多項式の次数をｍとすると、ｍビットのサイズであるので、例えば、２時間のコンテンツに対しては、初期値表は７２００＊ｍビットとなる。ストリームの途中から再生する場合、フレームアドレスとかタイムコードなどにより、現在のフレームが最初から何フレーム目であるかが容易に分かるので、初期値表から最適な初期値を選択し乱数発生器に設定すれば、極僅かなステップ数で乱数発生器を所望の状態にもっていくことが可能となる。

【００２７】このようにして、ストリームを部分的に暗号化し、かつ暗号化されているフレームであるか否かを示すフラッグ情報などをストリーム内に設けない方法でも、ストリームの任意の位置よりの再生が可能となる。なお、これら複数の初期値（初期値表）を受信側へ伝送するとき、そのまま伝送してもよいが、暗号化して伝送した方がより安全であることは確かである。

【００２８】以上の説明は、ストリームを部分的に暗号化し、かつ暗号化されているフレームであるか否かを示すフラッグ情報などをストリーム内に設けない伝送方法において、ストリームの途中から再生することを容易に可能とするために、送信側より乱数発生のための初期値表を伝送するという方法を紹介した。

【００２９】正規のユーザーである受信側（再生側）で乱数発生のための生成多項式が事前に分かっている場合には、伝送ストリームの再生に先立って初期値表を作成することが可能である。或いは、初期値表でなく乱数値そのものを作成することも可能である。というのは、乱数値は「０」か「１」の１ビットであるので、総フレーム分の乱数表を作成しても実現可能なサイズである。例えば、２時間のコンテンツで、フレーム周波数を１００Ｈｚとすると、総フレーム数は７２００ｘ１００＝７２０ｋビット＝９０ｋバイトとなる。

【００３０】一方、前述した初期値表の場合には、生成多項式の次数ｍ＝２０とし、１００フレーム毎の初期値表を作成しようとすると、７２００ｘ１００ｘ２０／１００ビット＝１８ｋバイトとなる。受信側（再生側）でのメモリーサイズの面からすると、初期値表を伝送或いは作成した方が優れているが、受信側で生成する総フレームに対応した乱数表の方が使い勝手に優れていると思われる。いずれにしても、不正使用に対する安全強度を確保しつつ、伝送ストリームの途中からの再生を容易に行える。

【００３１】ここで、上述した伝送ストリームの再生方法（受信方法）については次のような方法が考えられる。

（イ）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されたストリームを再生する暗号化情報再生方法であって、前記所定の生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

（ロ）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報が付加されたストリームを再生する暗号化情報再生方法であって、前記生成多項式暗号化情報の暗号を解き、得られた前記生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

（ハ）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の初期値の情報が暗号化された初期値暗号化情報とが付加されたストリームを再生する暗号化情報再生方法であって、前記生成多項式暗号化情報の暗号を解き前記生成多項式を復元すると共に、前記初期値暗号化情報の暗号を解き前記初期値を復元し、復元された前記生成多項式を用いて発生される乱数と、復元された前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

（ニ）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の乱数発生のための複数の初期値の情報が付加されたストリームを再生する暗号化情報再生方法であって、前記初期値の情報を再生して前記初期値を得、前記生成多項式を用いて発生される乱数と、再生した前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

【００３２】また、上記の再生方法を実現する暗号化情報再生装置としては、前記生成多項式暗号化情報の暗号を解き前記生成多項式を復元する手段と、前記初期値暗号化情報の暗号を解き前記初期値を復元する手段と、復元された前記生成多項式を用いて発生される乱数と、復元された前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定する手段と、フ

レーム毎の暗号化の有無が特定されたた後にその暗号化の有無の情報に基づき、ストリームの再生を行う手段をを備えた暗号化情報再生装置が考えられる。

【００３３】

【発明の効果】以上の通り、本発明によれば、音声や画像等のコンテンツ情報全体が暗号化されているのではなく部分的かつランダムに暗号化されており、しかも、暗号化されている部分がどの部分であるかを見つけ出し難くされている伝送ストリームを再生するので、コンテンツの不正使用に対する安全強度を高めた再生が行える。また、コンテンツ情報全体を暗号化せずに部分的かつランダムに暗号化している情報を再生するので、ある程度の品質での部分的な再生が自由に行え、ユーザーの購入意欲を増加させることにとって大変有利である。さらには、所定の生成多項式の乱数発生のための複数の初期値の情報が付加された伝送ストリームを再生する場合には、再生時において、不正使用に対する安全強度を確保しつつ、伝送ストリームの途中からの再生を容易に行える。

【図面の簡単な説明】

【図１】本発明における暗号化情報再生方法の一実施例で扱う伝送ストリームの暗号化処理を示す図である。

【図２】本発明における暗号化情報再生方法の一実施例で扱う伝送ストリーム生成のフローを示す図である。

【図３】従来の暗号化情報伝送方法を示す図である。

【図１】

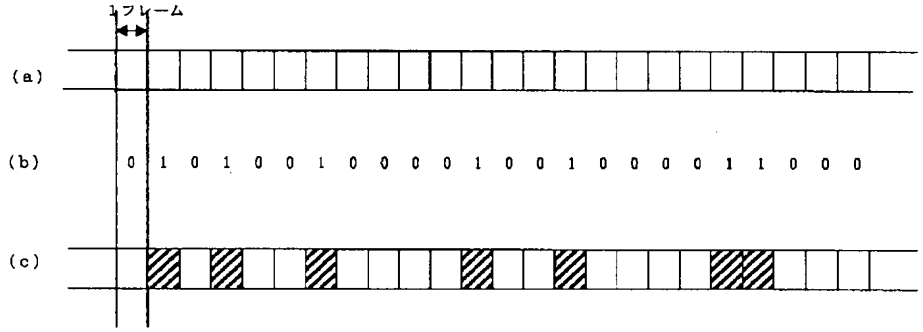


図1

【図2】

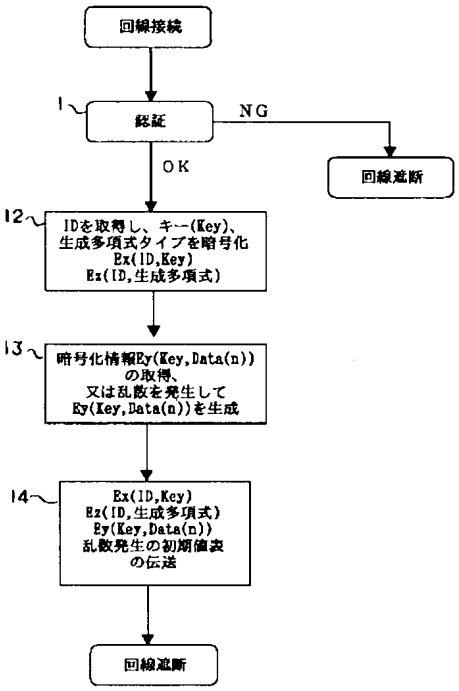

回線接続
1
認証
NG
回線遮断
OK
12
IDを取得し、キー(Key)、
生成多項式タイプを暗号化
Ex(ID,Key)
Ex(ID,生成多項式)
13
暗号化情報Ey(Key,Data(n))
の取得、
又は乱数を発生して
Ey(Key,Data(n))を生成
14
Ex(ID,Key)
Ez(ID,生成多項式)
Ey(Key,Data(n))
乱数発生の初期値表
の伝送
回線遮断

図2

【図3】

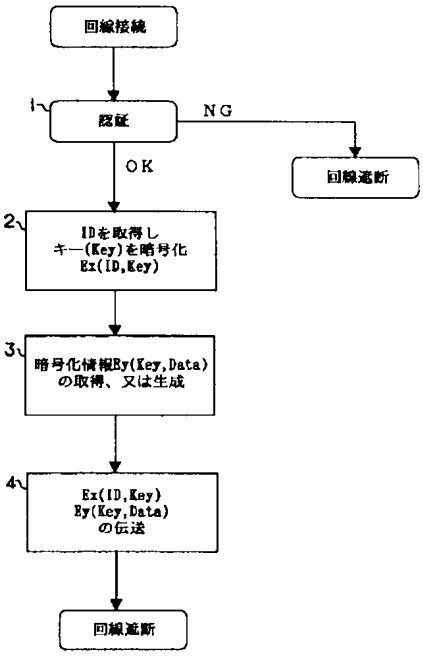

回線接続
1
認証
NG
回線遮断
OK
2
IDを取得し
キー(Key)を暗号化
Ex(ID,Key)
3
暗号化情報Ey(Key,Data)
の取得、又は生成
4
Ex(ID,Key)
Ey(Key,Data)
の伝送
回線遮断

図3